NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Boy brings gun to North Dakota school, shoots self. Residents of the southeastern North Dakota community of Fairmount were rattled after a high school boy brought a gun to class and shot himself. The school's principal said the boy survived what officials believe was a suicide attempt October 11. He said the boy did not threaten anyone else. The freshman boy was taken to a hospital. The principal said the boy was coherent. The principal said the K-12 school has approximately 110 students. The school was put into lockdown for about an hour after the incident, thn students were allowed to leave with their parents. Source: http://bismarcktribune.com/news/state-and-regional/boy-brings-gun-to-north-dakota-school-shoots-self/article_3e4777b0-13b5-11e2-975e-0019bb2963f4.html

Regional

(Minnesota) **After workplace shooting, Mpls. changes 911 procedures.** The city of Minneapolis is making a change with how it deals with 9-1-1 calls. It comes almost 2 weeks after Minnesota's worst workplace shooting, WCCO 4 Minneapolis reported October 10. At least four people called 9-1-1 from the scene of Accent Signage and never got through to a dispatcher. In all, seven people died in that attack September 27, including the gunman. The day of the attack, there were six 9-1-1 operators working alongside seven dispatchers. September 27, there were 65 calls from 4 p.m. to 5 p.m. — 16 were related to the shooting. In the police report, two Accent employees said they called 9-1-1 and it just kept ringing. Police arrived on scene 5 minutes after the first call to 9-1-1. The average response time to a call is more than 8 minutes. Now instead of a continued ring, if a call cannot be answered in 10 seconds, the caller will hear a recorded message urging the caller to stay on the line if it is safe to do so. Source: http://minnesota.cbslocal.com/2012/10/10/after-workplace-shooting-mpls-changes-911-procedures/

(South Dakota) **SD hospital being fined for radiation mishap.** The U.S. Nuclear Regulatory Commission (NRC) planned to fine a Sioux Falls, South Dakota hospital $11,200 for incidents in which a breast cancer patient suffered skin burns during treatment, the Associated Press reported October 4. The commission said the incident at Avera McKennan Hospital involved brachytherapy, which irradiates cancerous tumors inside the body. The agency said the patient's skin was exposed directly to radiation twice in January because of a computer programming error. Avera McKennan issued a statement saying it took the incidents seriously and cooperated with the NRC. The NRC said Avera McKennan has taken steps that provide —reasonable assurance that such an incident will not reoccur. Source: http://www.keloland.com/News/newsdetail6371.cfm/sd-hospital-being-fined-for-radiation-mishap/?id=138056

(Wyoming) **More data shows groundwater pollution from fracking.** The Summit County Citizens Voice reported October 9 that there is more evidence suggesting that fracking in Wyoming is polluting groundwater near the town of Pavilion. A U.S. Geological Survey (USGS) water quality sampling appeared to show similar results as an earlier Environmental Protection

Agency (EPA) study. The 2011 EPA sampling was one of the first to document hydrocarbons consistent with fracking fluid chemicals in drinking water wells and monitoring wells located near natural gas wells. The latest USGS study was conducted specifically to check EPA's results. To try and interpret the raw sampling data, the Sierra Club, Earthworks, and the Natural Resources Defense Council worked with a hydrologist and independent expert. The expert found that the USGS data supported EPA's initial findings. The USGS report found that thermogenic gas, which very likely comes from fracked deep-shale formations, continued to increase in a monitoring well. This evidence strongly suggests that as a result of fracking gas is seeping into Pavillion's water. Source: http://summitcountyvoice.com/2012/10/09/more-data-shows-groundwater-pollution-from-fracking/

(Wyoming) **Wyoming uranium project clears final hurdle.** Wyoming's Bureau of Land Management (BLM) released its decision on the proposed Lost Creek uranium project, World Nuclear News reported October 9. The decision is open to appeal, but represents the final regulatory approval needed for Ur-Energy to begin construction and operations. The BLM's decision authorizes Ur-Energy to recover uranium by pumping an oxidizing solution into a borehole to dissolve the uranium. Ur-Energy plans to start facility construction at Lost Creek in October. The company anticipated it would produce its first uranium in the summer of 2013. Ur-Energy said it expects the project to produce more than 7 million pounds of yellowcake at a rate of 1 million pounds per year. Source: http://www.world-nuclear-news.org/ENF-Wyoming_uranium_project_clears_final_hurdle-1010127.html

National

Nothing Significant to Report

International

'I will use a bomb to destroy an airplane,' computer virus says on victim's behalf. Japanese police arrested three people, accusing them of making online death threats. Later, however, investigators determined that a piece of malware may have actually posted the threats on their behalf. One of the suspects was detained after posting a message on a government site threatening to commit mass murder in a shopping area. An airline company was threatened via email that its planes would be bombed, a similar message was sent to the kindergarten attended by the children of the royal family, and a discussion board post mentioned blowing up a famous shrine. Authorities are investigating the connection between the malware and the threats, but security researchers reveal that the trojan in question, Backdoor.Rabasheeta, is capable of performing such tasks. Source: http://news.softpedia.com/news/I-Will-Use-a-Bomb-to-Destroy-an-Airplane-Computer-Virus-Says-on-Victim-s-Behalf-298664.shtml

Japan's TEPCO admits downplaying tsunami risk. The operator of the crippled Fukushima nuclear plant in Japan admitted October 12 it played down the risks of a tsunami to the facility for fear of the financial and regulatory costs. The report said that before the huge waves of March 2011 smashed into the plant, the company was aware defenses against natural disasters

were not sufficient but did not act because of the possible consequences. —There was a latent fear that plant shutdown would be required until severe accident measures were put in place, Tokyo Electric Power Company (TEPCO) said in a report. The company document, entitled —Fundamental Policy for the Reform of TEPCO Nuclear Power Organization , said insufficient planning was done to prepare for a natural disaster at the plant. Source: http://phys.org/news/2012-10-japan-tepco-downplaying-tsunami.html

Mexican troops arrest 2 in killing of U.S. border agent. Mexican troops have arrested two suspects in the killing of a U.S. Border Patrol agent and the wounding of a second officer in Naco, Arizona, Mexican security officials said October 3. The two suspects were detained in a Mexican military operation in the city of Agua Prieta, in Mexico's northern Sonora State, a few miles from the spot where the agent was shot dead October 2 while responding to a tripped ground sensor, a Mexican army officer told Reuters. A Mexican police official in Naco confirmed the arrests. Source: http://worldnews.nbcnews.com/_news/2012/10/03/14206322-mexican-troops-arrest-2-in-killing-of-us-border-agent?chromedomain=usnews&lite

Report says EU nuclear plants need better safety. The European Union (E.U.) energy commissioner said October 4 the cost of necessary improvements at the 145 nuclear reactors in the E.U. could be as high as $32 billion in coming years. An EU report said stress tests carried out in the wake of the March 2011 Fukushima accident in Japan showed that almost all the plants need safety improvements. Officials said earlier that the tests did not reveal the need to close any plants immediately. E.U. leaders agreed in 2011 to put the reactors through the toughest security checks possible to gauge their ability to withstand accidents and natural disasters. The energy commissioner said that —nearly everywhere there was potential for improvement to reach the highest level of safety, ranging from ensuring more time to react to an electricity blackout to adding more seismic equipment to detect earthquakes. The report criticized the authorities for not taking the latest standards into account to assess risks. For earthquake and flooding risk, standards now called for an assessment based on occurrences of the past 10,000 years, while many nuclear power plants use a shorter time frame. Equipment to fight severe accidents is not stored for quick retrieval in 56 percent of cases, and almost everywhere equipment to alert for earthquakes should be upgraded, or installed. In case of an electricity blackout, five reactors would not be able to cope for more than an hour without intervention. Source: http://www.foxnews.com/world/2012/10/04/report-says-eu-nuclear-plants-need-better-safety/

Banking and Finance Industry

SEC automating analysis of suspicious trading patterns. The Chairman of the Securities and Exchange Commission (SEC) said October 11 that the SEC is upgrading its investigative technology so it can identify —suspicious trading patterns and relationships among multiple traders and across multiple securities.'' She told the 2012 New England Securities Conference that the SEC will use —newly-developed analytics to spot abuses. A new Market Abuse Unit has spearheaded the analysis project for the Division of Enforcement. With the tool, —staff are able to search across this database to recognize suspicious trading patterns and identify

relationships and connections among multiple traders and across multiple securities, generating significant enforcement leads and investigative entry points,‘‘ according to the enforcement‘s division director. The agency also has put in place an Aberrational Performance Inquiry team that focuses on identifying hedge fund managers that may be engaging in fraudulent practices. The agency is also using an —e-discovery system to make wide searches of data produced for the agency by the securities industry to find —needles that might have been missed or overlooked.‘‘ That system will be integrated with other tools, including technology that allows phonetic searches of voice recordings, to find leads. Source: http://www.tradersmagazine.com/news/sec-automates-identification-suspicious-trading-110401-1.html?pg=1

Experts: Banks should review authentication procedures to prevent trojan attacks. According to a report released by security firm RSA, U.S. financial institutions should expect to become the targets of cyberattacks. The firm was not referring to the recent distributed denial-of-service (DDOS) attacks launched by hackers, but the campaign called Project Blitzkrieg, Softpedia reported October 12. Project Blitzkrieg is said to rely on a trojan called Gozi Prinimalka to intercept wire transfers made by the banks‘ customers with the purpose of emptying their accounts. To ensure success, the initiators want to target 30 unnamed banks with the help of 100 botmasters that could help in sustaining the attacks. Researchers from information security firm Solutionary once again highlighted that this operation leverages the weak state of security surrounding financial institutions, especially those from the United States. —Solutionary highly recommends banks review authentication procedures for wire transfers a research analyst at Solutionary‘s Security Engineering Research Team explained. The expert warned that directly or indirectly this campaign will result in a DDOS attack and regular users, as well as the targeted firms, should be prepared to handle it. That is because the botnets utilized in massive DDOS attacks often composed of work or home computers. Source: http://news.softpedia.com/news/Experts-Banks-Should-Review-Authentication-Procedures-to-Prevent-Trojan-Attacks-298953.shtml

SunTrust the latest victim in cyber attack saga. SunTrust seemed to be the latest bank targeted with a denial of service attack October 10 in a chain of cyber attacks that hit Capital One October 9 and other major Wall Street institutions in September. The hacking group in a blogpost October 8 said it would target Capital One October 9, regional bank SunTrust October 10, and Regions Financial October 11. A handful of users reported on Twitter and SiteDown.co they were having issues accessing SunTrust‘s e-banking Web site. That is different from some of the earlier attacks where customers could not access the main customer Web site altogether. When attempting to log on, some customers complained of receiving one of two error messages: —Server Unavailable or —Server is too busy . —We have seen increased traffic today and have experienced some intermittent service availability, a SunTrust spokesperson said. October 9, SunTrust said that it was —aware of the threat and was working to mitigate any disruption to clients should an attack occur. The group threatened to pursue more cyber attacks the week of October 15 and has long said it will not stop until a video mocking the Islam religion first posted to YouTube is removed from the Internet. Source:

http://www.foxbusiness.com/technology/2012/10/10/suntrust-may-be-latest-victim-in-cyber-attack-saga/

Fraudulent e-mails claiming to be from the FDIC. The Federal Deposit Insurance Corporation (FDIC) has received numerous reports of fraudulent emails that have the appearance of being sent from the FDIC, according to a notice released October 3. While the emails exhibit variations in the —Subject lines, the messages are similar. They all make reference to the suspension of recipient's ability to conduct transfers via ACH and/or wire transfer. The emails then encourage recipients to install a software update by clicking on a link provided. They then say that functionality will be restored once the software update is installed. The emails and the link provided are fraudulent. Recipients should consider the intent of these emails to load malicious software on the recipient's computer, or to collect personal or confidential data. Recipients should not click on the link provided. The FDIC does not send unsolicited emails to consumers or business account holders. Source: http://content.govdelivery.com/bulletins/gd/USFDIC-55ee11

Cybercrime gang recruiting botmasters for large-scale MiTM attacks on American banks. A slew of major American banks may soon have to brace themselves for a large-scale coordinated attack bent on pulling off fraudulent wire transfers, ThreatPost reported October 4. RSA's FraudAction research team has been monitoring underground chatter and has put together various clues to deduce that a cybercrime gang is actively recruiting up to 100 botmasters to participate in a complicated man-in-the-middle hijacking scam using a variant of the proprietary Gozi Trojan. This is the first time a private cybercrime group has recruited outsiders to participate in a financially motivated attack, said a cybercrime communications specialist for RSA FraudAction. The attackers are promising their recruits a cut of the profits, and are requiring an initial investment in hardware and training in how to deploy the Gozi Prinimalka Trojan. Also, the gang will only share executable files with their partners, and will not give up the Trojan's compilers, keeping the recruits dependent on the gang for updates. With this kind of scale, banks could be facing up 30 times the number of compromised machines and fraudulent transfers as the average attack, if the campaign is successful. As many as 30 banks have been targeted, many of them well known and high profile. RSA said the gang is targeting American banks because of past success in beating their defenses, as well as a lack of two-factor authentication required for transfers. Source: http://threatpost.com/en_us/blogs/cybercrime-gang-recruiting-botmasters-large-scale-mitm-attacks-american-banks-100412

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(Colorado) **Aurora shooting suspect faces new charges.** Prosecutors October 11 added 14 counts of attempted murder to the charges against the suspect in the July 20 Aurora, Colorado

theater shooting. Prosecutors also amended five other counts that the man already faced. Details about the new charges were not made public. The man is accused of donning body armor and killing 12 people and injuring 58 after opening fire in a movie theater during a crowded midnight film premiere. He already faces multiple murder and attempted-murder charges. Source: http://www.usatoday.com/story/news/nation/2012/10/11/holmes-aurora-murder-theater-batman/1627229/

Communications Sector

A better reason to avoid Huawei routers: Code from the '90s. A security researcher has a more compelling reason to avoid routers from Huawei Technologies than fears about their ownership. While the company blasted for its opaque relationship with China's government in a U.S. intelligence report released October 8, a bigger worry for some is what is inside its routers. —The code quality is pretty much from the _90s, said the researcher, who analyzed the software inside Huawei's home and enterprise routers, and runs Recurity Labs, a security consultancy. He will speak October 11 at the Hack in the Box security conference and discuss the vulnerabilities he and a fellow researcher disclosed earlier in 2012 along with an overview of Huawei's security. When the researcher began looking at Huawei's routers, the firm did not have a prominent product security team, he said. However, since he and his colleague detailed vulnerabilities in the firmware of Huawei's AR18 series routers, which are meant for homes, and its AR29 series routers, intended for small enterprises, at the Defcon conference in July, —they seem to be trying to ramp up product security in a visible way right now, he said. Source: http://www.computerworld.com/s/article/9232229/A_better_reason_to_avoid_Huawei_routers_Code_from_the_90s

Telecom vendors Huawei, ZTE, pose cyber-espionage threats, lawmakers conclude. Two top telecom infrastructure vendors from China, Huawei, and ZTE, pose potential cyber-espionage threats, according to a panel of U.S. lawmakers on intelligence, Infosecurity reported October 8. After an 11-month investigation, the U.S. House of Representatives' Permanent Committee on Intelligence suggested that telecom networks built on Huawei and ZTE gear could provide a way for the Chinese government to bake in listening vectors, for instance. There is a "heightened threat of cyber espionage and predatory disruption or destruction of US networks if telecommunications networks are built by companies with known ties to the Chinese state, a country known to aggressively steal valuable trade secrets and other sensitive data from American companies," the report said. The panel recommended that American telcos, cable MSOs, satellite companies, wireless operators, and broadband providers should consider other vendors going forward when building out or expanding networks. And, sensitive government systems should exclude Huawei or ZTE equipment or component parts — Huawei in particular has a large enterprise IT division that could supply federal and State networks. And, it said that it would seek to block mergers or acquisitions involving Huawei and ZTE due to national security concerns. Source: http://www.infosecurity-magazine.com/view/28672/telecom-vendors-huawei-zte-pose-cyberespionage-threats-lawmakers-conclude/

Sprint fixes network disruption in Pacific Northwest. Two fiber cuts to Sprint Nextel Corp.'s wireless network affected Pacific Northwesterners trying to make phone calls, use data on their smartphones, and even catch flights October 8. All services were restored by October 8, according to Overland Park-based Sprint. The first cut happened October 7 or October 8, botching service to customers between Chicago and Milwaukee. A Sprint spokeswoman said the incident was tied to work at a railroad involving non-Sprint employees. A second cut happened again October 8, somewhere between Tacoma, Washington, and Portland, Oregon, disrupting voice and data services for customers between northern California, parts of Oregon, and parts of Washington. Sprint has not determined the cause of the second cut, which slowed the terminal check-in process for Sprint customer Alaska Airlines October 8, leading to significant flight delays. Alaska Airlines, which uses Sprint's data services, had to manually check in passengers until the fiber lines were repaired and services were restored, a spokeswoman for Sprint said. Source: http://www.bizjournals.com/kansascity/news/2012/10/08/sprint-fixes-network-disruption-in.html

CRITICAL MANUFACTURING

Sharper Image USB wall chargers recalled by Atomi due to fire and burn hazards. The U.S. Consumer Product Safety Commission, in cooperation with Atomi of New York City, October 10 announced a voluntary recall of about 80,000 Sharper Image USB wall chargers. Consumers should stop using recalled products immediately unless otherwise instructed. The chargers can overheat and smoke, posing fire and burn hazards. Atomi received 13 reports of the chargers overheating, smoking, and producing acrid smells. The chargers were sold at Burlington Coat Factory, Tuesday Morning, and TJ Maxx stores, and on various Web sites from October 2011 through September 2012. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml13/13007.html

Feds investigate steering in Hyundai Santa Fe. U.S. safety regulators are investigating a steering problem in Hyundai Santa Fe sport utility vehicles (SUV), the Associated Press reported October 12. The NationalHighway Traffic Safety Administration (NHTSA) said a fastener can come loose, causing the steering shaft to come apart and drivers to lose control of the vehicle. The investigation covers about 70,000 Santa Fes from the 2011 model year. It will determine if the problem is bad enough for Hyundai to recall the SUVs. NHTSA said one driver complained about a complete loss of steering. Hyundai also received a complaint that a loose bolt caused a similar problem. Source: http://mdjonline.com/view/full_story/20471817/article-Feds-investigate-steering-in-Hyundai-Santa-Fe-?instance=secondary_story_left_column

Feds studying problems with Ford Escape throttles. U.S. safety regulators are looking into throttle problems in older Ford Escapes at the request of a consumer group, the Associated Press reported October 5. The nonprofit North Carolina Consumers Council asked federal regulators to investigate two complaints from drivers who say the small SUV stalled or surged forward. The government will look at 1.6 million Escapes from the 2005 to 2012 model years. If the National Highway Traffic Safety Administration (NHTSA) decides to launch a formal investigation, it could lead to a recall of some of the popular SUVs. In the latest case, released by NHTSA October 5, the consumers council said Ford sent a number of advisories to dealers

about Escapes stalling and surging. Technical service bulletins were sent out to help mechanics spot problems and fix them. The Escape has been recalled four times since July, with the 2013 version responsible for three of the recalls. Source: http://www.myfoxal.com/story/19744171/feds-studying-problems-with-ford-escape-throttles

Over 40,000 vehicles involved in Chrysler recall. Tens of thousands of Chrysler pick-up trucks are involved in a national recall. Chrysler announced nearly 45,000 vehicles could have rear axle problems, the Associated Press reported October 6. 2009-2010 models of the Ram 1500 and Dodge Dakota could have a lack of an adhesive, which could cause the rear axle pinion nut to loosen. If that nut does become loose, the axle can lock up, and the driver could lose control and crash. According to Chrysler, there have been 15 reports of axle failure which resulted in 3 minor injuries. The recall involves 44,300 vehicles built between July and November of 2009. Chrysler will notify owners of the recall beginning in November. Dealers will install a retainer to secure the pinion nut free of charge. Source: http://www.newsnet5.com/dpp/money/consumer/over-40000-vehicles-involved-in-chrysler-recall

Honda recalls 2002-2006 CR-V for fire risk. Honda and the National Highway Traffic Safety Administration (NHSTA) announced October 6 that Honda Motor Co. is recalling CR-V crossovers from the 2002 to 2006 model years because an electrical switch in the driver's side door could melt and cause a fire. The problem involves around 268,000 vehicles. Honda said rain or other liquids could enter through a driver's open window and damage the master power switch on the door. If that happens, the switch could overheat and melt, causing a fire. NHTSA said owners should park CR-Vs from those model years outside until the recall is performed to avoid any property damage from a fire. A fire could start even when the ignition is off and the CR-V is parked. The company will begin contacting owners in November and will repair the vehicles for free. Honda will install a cover plate inside the switch to prevent any liquid from coming entering the vehicle. Source: http://www.kypost.com/dpps/news/national/honda-recalls-2002-2006-cr-v-for-fire-risk_7912028

Safety agency investigating Honda Pilot, Odyssey. The U.S. National Highway Traffic Safety Administration (NHTSA) is investigating complaints that Honda Odyssey Minivans and Pilot sport utility vehicles (SUV) can roll away after drivers remove the ignition key, the Associated Press reported October 5. The probe affects more than 577,000 vehicles from the 2003 and 2004 model years that have automatic transmissions. The mechanism that locks the key in the ignition can fail. When that happens, drivers of the vans and SUVs are able to remove keys without shifting into park. Some have left the vehicles, and the vans or SUVs have rolled off. Owners have filed 43 complaints with NHTSA, including 16 that resulted in crashes. Two people reported injuries. Source: http://www.wbay.com/story/19744062/safety-agency-investigating-honda-pilot-odyssey

GE recalls front load washers due to injury hazard. The U.S. Consumer Product Safety Commission, in cooperation with GE Appliances, October 3 announced a voluntary recall of about 62,000 GE Profile Front Load Washers. Consumers should stop using recalled products

immediately unless otherwise instructed. The washer's basket can separate during use and break the washer's top panel, posing an injury hazard to consumers. GE has received 19 reports of washer baskets separating, including 10 reports of top panel breakage. The dishwashers were sold at Best Buy, Lowe's, Sears, Home Depot and other department and retail stores nationwide, from July 2008 to August 2011. Consumers should immediately stop using the recalled washers and contact GE for a free repair. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml13/13003.html

Defense/ Industry Base Sector

(Tennessee) **ORNL locked down Sunday as officials investigate security concern.** Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee, was locked down for more than four hours October 7 as officials investigated a security-related concern that turned out to be unsubstantiated, a spokesman said. Officials took the proper precautions and stopped people from entering or leaving the lab during the lockdown, according to the ORNL communications director. The ORNL Communications Director said that there are about 100 support staff members at ORNL on Sundays, including at the Spallation Neutron Source and High Flux Isotope Reactor, and possibly another 50 researchers at the lab. Source: http://oakridgetoday.com/2012/10/08/ornl-locked-down-sunday-as-officials-investigate-security-concern/

Emergency Services

CO2 exposure in public places increasing danger for emergency responders. New generation technology that delivers Carbon dioxide (CO2) to soda fountains in restaurants and other commercial applications could be a hidden danger to emergency responders, warned a memo circulated to emergency responders during the summer of 2012 by the Los Angeles Joint Regional Intelligence Center, Government Security News reported October 5. The "Unclassified, For Official Use Only (U//FOUO)" memo circulated to emergency responders by the fusion center in July and made available on the Public Intelligence open source Web site October 4, notes that within the past years, first responders and members of the public have had numerous issues with CO2 exposure in public places. The memo said first responders and members of the public have died of asphyxiation, -or fallen ill, following accidental inhalation of concentrated carbon dioxide in public locations. It said at least two recent emergency response incidents resulted from significant gas leaks caused by the failure of liquid CO2 lines connected to beverage dispensers in commercial facilities. Source: http://www.gsnmagazine.com/node/27530?c=disaster_preparedness_emergency_response

(California) **Sinaloa cartel leader tied to drug tunnels.** An indictment by U.S. authorities tied a top Mexican cartel member to two of the largest drug tunnels ever found under the San Diego-Tijuana border, an indictment indicated, United Press International reported October 4. Federal prosecutors in San Diego said the cartel member who was arrested in Mexico on money-laundering charges in January and faces extradition proceedings, is the highest-ranking member of the Sinaloa drug cartel ever charged in construction of underground tunnels, the Los Angeles

Times reported October 4. The 13-count federal indictment was handed down by a grand jury in San Diego in February and unsealed October 3. Prosecutors allege the cartel member oversaw construction and operation of a 2,200-foot-long tunnel discovered in November 2010, and a similar underground passageway found in 2011. Prosecutors said he received frequent updates on construction work, controlled drug flow, and directed other traffickers to use the tunnels. Source: http://www.upi.com/Top_News/US/2012/10/04/Sinaloa-cartel-leader-tied-to-drug-tunnels/UPI-37951349350206/?spt=hs&or=tn

ENERGY

(Vermont) **Copper thieves target substations.** Green Mountain Power (GMP) said copper thefts from its electric substations all over Vermont are reaching the point where thieves are threatening the lives of utility workers and the nearby public, WCAX 3 Burlington reported October 7. The utility said that over the past two months four sub-stations have been vandalized by copper thieves. GMP stated at one substation the thieves cut the lock to the gate, which created a public hazard by allowing access to a dangerous facility. Also, power to customers must be cut to make the repairs following the break-ins. Source: http://www.wcax.com/story/19758861/copper-thieves-target-substations

(Texas) **Dallas area earthquakes were caused by fracking: Geophysicists.** Three earthquakes that hit a Dallas suburb the week of October 1 could be connected to fracking operations, according to a local geophysicist who studies earthquakes in the region. RT reported that the earthquakes were considered minor, with the biggest one registering a 3.4 on the Richter scale. A senior scientific researcher and associate director at the University of Texas believed the earthquakes were related. In a study published in the journal Proceedings of National Academy of Sciences in August 2012, he found that 67 earthquakes occurred between November 2009 and December 2011 within a 43-mile grid where fracking occurs over the northern Texas Barnett Shale formation. Twenty-four of the earthquakes, where the epicenter could be reliably mapped, occurred within 2 kilometers of the injection wells for wastewater disposal from fracking. Source: http://www.homelandsecuritynewswire.com/dr20121008-dallas-area-earthquakes-were-caused-by-fracking-geophysicists

(West Virginia) **Four charged in theft of copper wire from power stations.** Four people have been charged in the theft of more than 400 pounds of copper wire from multiple electric power substations in Berkeley County, West Virginia since August, according to county court records. The four were arraigned the week of October 1 on charges of conspiracy to commit breaking and entering, court documents said. The charges filed against the defendants stem from police investigation of five cases of copper ground wire theft at four Potomac Edison substations, according to a Berkeley County sheriff's deputy lieutenant. Charges have yet to be filed in three other cases of copper wire theft from substations in Berkeley County. Another case in Morgan County also is pending, he said. The value of the copper stolen was calculated to be about $1,392, but the cost of repairing the damage to the substation fence as well as the power company's equipment exceeded $30,000. The stolen copper wire was sold at multiple scrap metal businesses in the area, according to court documents. Source: http://www.herald-

mail.com/news/tristate/hm-four-charged-in-theft-of-copper-wire-from-power-stations-20121003,0,5989234.story

Food and Agriculture

Dean Foods Company of California and Meadow Gold Dairy Conduct voluntary recall of two Albertsons brand ice cream varieties. October 10, the Dean Foods Company facility in Buena Park, California and Meadow Gold Dairy processing facility in Orem, Utah, announced a voluntarily recall of two ice cream varieties manufactured for Albertsons supermarkets. The products contain a peanut butter ingredient supplied by Sunland, Inc. which may be contaminated with Salmonella. The recalled products include the —Peanut Butter Cup and —Peanut Butter Chocolate flavors that were sold in 1.5-quart cartons in Albertsons stores with plant codes 49-11 or 06-20. The product was sold between March 26, 2010 and September 25, 2012, in California, Idaho, Montana, Nevada, North Dakota, Oregon, Utah, Wyoming, and Washington. Source: http://www.fda.gov/Safety/Recalls/ucm323388.htm

Harry and David, LLC expands its voluntary recall of peanut butters, peanut spreads, and related products due to potential health risk based on the expanded recall by Sunland, Inc. October 8, Harry and David, LLC expanded its recall of peanut butters, peanut spreads, and related products. Harry and David's recall is in response to an expansion of Sunland, Inc.'s recall of products manufactured in its peanut butter plant after March 1, 2010. The affected products are 12-ounce jars of Harry & David brand Crunchy Almond and Peanut Butter, Creamy Banana Peanut Spread, Creamy Caramel Peanut Spread, and Creamy Raspberry Peanut Spread with best by dates of March 1, 2011 through September 24, 2013. The recall also includes the following multi-component food items which included the above-named peanut butter products as components: Harry & David Apple Snack Box, Wolferman's Bee Sweet Gift Basket, Hearty Snack Gift Basket, All-Day Assortment Gift Basket, and Father's Day Basket. Products were sold nationwide through Harry & David and Wolferman's catalogs and Web sites, as well as through Harry & David stores, between May 26, 2010 and September 25, 2012. Source: http://www.fda.gov/Safety/Recalls/ucm323010.htm

Sunland, Inc. announces voluntary expansion of ongoing recall to include all products manufactured in its peanut butter plant after March 1, 2010 due to possible health risk. October 4, Sunland, Inc. announced a voluntary expansion of its ongoing recall of all products manufactured in its peanut butter plant because they are potentially contaminated with Salmonella, the U.S. Food and Drug Administration reported. The expansion includes all products manufactured after March 1, 2010, and added 49 products whose best-if-used-by dates have not expired. The expanded recall also adds 90 products consumers may still have in their homes but have expired. Distribution of many of the newly recalled products was discontinued some time ago. The expansion covers all previously identified peanut butter, almond butter, cashew butter, tahini, and roasted blanched peanut products. The new product categories are several varieties of flavored butters and spreads, including Thai Ginger Butter, Chocolate Butter, and Banana Butter. As of September 25, the Centers for Disease Control and Prevention reported a total of 30 illnesses in 19 States. The products, distributed under the

Sunland's own label and under other brand names, were distributed nationally to numerous large supermarket, grocery, and retail chains. The products were also available for purchase on the Internet. Source: http://www.fda.gov/Safety/Recalls/ucm322747.htm

FDA finds salmonella, unclean conditions at farm. A federal inspector found two strains of salmonella and unclean conditions at an Indiana cantaloupe farm's fruit-packing plant during visits following a deadly outbreak linked to its melons, the Associated Press reported October 3. The U.S. Food and Drug Administration (FDA) posted a report on its Web site of the inspector's findings during mid-August visits to Chamberlain Farm Produce Inc., in Owensville. The report includes improperly cleaned equipment and algae growing in standing water beneath conveyer belts in the plant. One of the two salmonella strains was found on cantaloupes that were processed and boxed. The FDA said the farm is the source of at least some of the salmonella outbreaks that sickened 270 people in 26 States during the summer. Officials said 101 people were hospitalized, and 3 deaths were reported in Kentucky. Source: http://www.usatoday.com/story/news/health/2012/10/03/fda-farm-salmonella-outbreak-unclean/1610277/

Costco recalls smoked salmon sold to quarter of a million customers. Costco Wholesale — the only U.S. carrier of the European smoked salmon linked to hundreds of Salmonella illnesses in the Netherlands — issued a recall of the fish October 1, using its automated system to call the nearly 250,000 consumers who purchased the product over the past month. The smoked salmon was sold across the United States under two brands: Foppen and Kirkland Signature. Both products were manufactured by Foppen, a Netherlands-based company. The Foppen-branded fish was processed at a plant in Greece, while the Kirkland Signature-branded fish came from a plant in the Netherlands, said Costco's director of food safety. So far, only the Foppen smoked salmon from the Greek facility tested positive for Salmonella; the Kirkland Signature fish was recalled out of extra precaution, the director said. Source: http://www.foodsafetynews.com/2012/10/costco-recalls-smoked-salmon-sold-to-quarter-of-a-million-customers/

Government Sector (including Schools and Universities)

(Oklahoma) **OKCPS tightens security after middle school stabbing.** October 10, leaders of Oklahoma City Public Schools (OKCPS) said they tightened security across the district after a stabbing at Roosevelt Middle School. A 7th grade student got through metal detectors with the knife he used to stab another student at lunch October 8. All secondary campuses in the district have walk-through metal detectors, but police reports show the student at Roosevelt got through by putting the knife in his shoe. —We've identified what problem we've had in our process and corrected it, not only at Roosevelt but all of our secondaries, said the OKCPS chief operating officer, who heads security at the district's schools. He noted no security system is perfect. —You've got to understand we're wanding and scanning over 20,000 secondary students on a daily basis, so something like this happening is an anomaly. Police reports also

showed the attacking student had a box blade hidden in his pants. He faces a charge of assault and battery with a deadly weapon, and carrying a weapon on school grounds. That student was suspended from school for a year. Source: http://www.news9.com/story/19789017/okcps-tightens-security-after-middle-school-stabbing

Think tanks hit by hackers from China, other nations. USA Today reported October 4 that American think tanks are key targets in a "furious wave of cyber-espionage" aimed at U.S. Government and business by China and other countries, according to the chairman of the House Intelligence Committee. A Michigan congressman said the hacking is part of a campaign by China and other nations to obtain valuable information on a number of fronts, from policy deliberations and pending litigation, to national defense and private product development. A senior fellow and director of technology and public policy at the Center for Strategic and International Studies, said that during the transition to the U.S. President's administration in 2008 and 2009 some people moving from think tanks and the private sector into the administration had their email accounts hacked. He said the hackers were looking for information to help build profiles on those who were about to serve in the government. The FBI's former top cyber-security official said overall cyber-attack complaints reported to U.S. authorities were increasing by 20 percent annually. He said that think tanks, consulting organizations, and law firms have long been prized targets of foreign espionage operations. Source: http://www.usatoday.com/story/news/nation/2012/10/04/think-tanks-cyberattacks-china-hacking/1600269/

Sensitive documents left behind at U.S. diplomatic post in Libya. More than 3 weeks after attacks in Benghazi killed the U.S. ambassador to Libya and three other Americans, sensitive documents remained only loosely secured in the wreckage of the U.S. mission, offering visitors easy access to delicate information about American operations in Libya, the Washington Post reported October 3. Sensitive documents were among the items scattered across the floors of the looted compound when a Washington Post reporter and an interpreter visited October 3. No government-provided security forces are guarding the compound, and Libyan investigators have visited just once, according to a member of the family who owns the compound and who allowed the journalists to enter October 3. —Securing the site has obviously been a challenge, a deputy spokesman at the State Department said in response to questions about conditions at the Benghazi compound. —We had to evacuate all U.S. government personnel the night of the attack. After the attack, we requested help securing the site, and we continue to work with the Libyan government on this front. Source: http://www.washingtonpost.com/world/middle_east/sensitive-documents-left-behind-at-american-mission-in-libya/2012/10/03/11911498-0d7e-11e2-bd1a-b868e65d57eb_story.html

Information Technology and Telecommunications

Average insurance cost per data breach rises to $3.7M: Study. The average insurance cost per computer data breach incident increased from $2.4 million in 2010 to $3.7 million in 2011, according to a new NetDiligence study. Based on claims submitted in 2011 for incidents between 2009 and 2011, the average number of records exposed decreased 18 percent to 1.4

million, according to the study. A typical breach ranged from $25,000 to $200,000 in insurance costs. Legal damages stemming from data breaches represented the bulk of insurance costs, at an average of $582,000 for legal defense costs and an average of $2.1 million in settlements costs, compared with $500,000 and $1 million, respectively, in 2010. Source: http://www.businessinsurance.com/article/20121009/NEWS07/121009907

New security threat at work: Bring-your-own-network. Even as IT pros wrestle with the bring-your-own-device (BYOD) trend, corporate security is being further complicated by another emerging trend: bring your own network (BYON). BYON is a byproduct of increasingly common technology that allows users to create their own mobile networks, usually through mobile wireless hotspots. Security professionals say BYON requires a new approach to security because some internal networks may now be as insecure as consumer devices. An attorney with the law firm Much Shelist said BYON represents a more dangerous threat to data security than employees who bring their own smartphones or tablets into the office. —The network thing blows this up completely, because it takes the data out of the network the company protects, he said. Source: http://www.computerworld.com/s/article/9232302/New_security_threat_at_work_Bring_your_own_network

Bing is the most heavily poisoned search engine, study says. Bing search results are more affected by poisoning than those of other search engines, according to a study by SophosLabs. Search engine poisoning attacks are designed to skew results so that dodgy sites — anything from malware infected Web sites to payday loan sites — appear prominently in the index of sites related to popular search terms. In many cases, the tactic is so successful that malware sites appear in the first page of results for popular search terms, sometimes much higher than legitimate Web sites. More recently, miscreants began trying to manipulate image search results. Source: http://www.theregister.co.uk/2012/10/08/bing_worst_search_poisoning/

New TDL4 rootkit successfully hiding from AV. A new variant of TDL4 was identified, and it is now ranked as the second most prevalent malware strain within 2 months since its detection. The characteristics are similar to the iteration of the TDL4 rootkit, detected by Damballa in September. Damballa detected the malware through its network behavioral analysis software, which detected the generated domain names the new variant apparently uses for command-and-control communication. Since Damballa could only determine the existence of the new malware by looking for domain fluxing, it was concluded that no binary samples of the new malware were identified and categorized by commercial antivirus products operating at the host or network levels. HitmanPro, however, detected Sst.c — also known as Maxss — a modification of the TDL4 strain, and it is spreading fast. This new variant is capable of infecting the Volume Boot Record (VBR) (also known as Partition Table), and commercial antivirus products are unable to detect it, let alone remove the malware. The vice president and GM Wave Systems EMEA provided the following commentary: “Following the success of TDL4, hackers have been able to use the rootkit to develop new variants that continue to go undetected by antivirus. The latest iteration, dubbed Sst.c, infects the Volume Boot Record.” Without embedded hardware security to detect anomalies of behavior in the boot process, it

starts to cause havoc damaging the network. It also reduces the window of detection for the enterprise to contain the threat. Source: http://www.net-security.org/malware_news.php?id=2288

Bogus Skype password change notifications lead to phishing. Bogus emails supposedly sent by Skype are targeting users of the popular VoIP service, saying their Skype password was —successfully changed. Users who have not recently initiated the password change themselves are in danger of believing their account is being hijacked and following the offered links. Those that do will be faced with a spoofed Skype login page that sends the entered login credentials to the scammers behind the phishing attempt. Users are advised to always log into the legitimate online services only via the official login page. Source: http://www.net-security.org/secworld.php?id=13728

Adobe revokes code signing certificate for software signed after July 10, 2012. October 4, Adobe revoked the compromised code signing certificate that was used to sign several malicious applications. Updates signed with a new certificate were issued. The revoked certificate was used to sign software code after July 10, 2012. According to Adobe, the Windows platform and three Adobe AIR applications – Acrobat.com desktop services, Adobe Story AIR applications, and Adobe Muse – for both Windows and Mac are affected. Source: http://news.softpedia.com/news/Adobe-Revokes-Code-Signing-Certificate-for-Software-Signed-After-July-10-2012-297123.shtml

Trojan disguised as image delivered via Skype messages. A spamming campaign that surfaced in the last few days is being propagated via compromised Skype accounts. The offered links do not lead to an image, but to a malicious executable (skype_02102012_image.exe) posing as one. —Running the file will cause it to self delete and the infected PC will begin making DNS requests to a number of URLs, including a .pl, a .com and a .kz - we also saw references to IRC channel names in the network traffic and are investigating further, said a researcher from GFI. Source: http://www.net-security.org/malware_news.php?id=2285

Blackhole responsible for a third of drive-by download attacks. According to new research, malware created using the Blackhole toolkit can be found on nearly one third of all malicious Web links circulating in the wild. A team comprised of researchers at Google, the International Computer Science Institute, and several leading U.S. universities warned that so-called drive-by downloads are becoming cyber criminals' attack of choice. The team studied more than 77,000 malicious URLs identified using Google's Safe Browsing — a tool Google uses to identify sites carrying malicious payloads. They then attempted to analyze the code these sites were dispensing, analyzing the malware being distributed and the tools used to create it. Nearly half of all Web pages serving exploits were based on two toolkits: Blackhole and Incognito. Source: http://www.v3.co.uk/v3-uk/the-frontline-blog/2214082/blackhole-responsible-for-a-third-of-driveby-download-attacks

Malicious spam campaign targets QuickBooks users. Intuit-themed malicious spam campaigns appear every few months, given that the company's tax preparation, accounting, financial

management, and billing software and services are extremely popular in the United States and Canada. The latest one, spotted by GFI Software, tries to attract the users of Intuit's QuickBooks — accounting software marketed to small business owners — with an offer of free shipping when ordering tax forms. For the recipients who click on them, the embedded links lead not to the ordering form, but to a page that shows a —Connecting to server... message and eventually redirects them to another page hosting the Blackhole exploit kit. Source: http://www.net-security.org/malware_news.php?id=2282

National Monuments and Icons

(Oregon; Washington) **Northwest wildfires have burned record number of acres in 2012.** The U.S. Forest Service and Bureau of Land Management (BLM) said 2012 has been the worst fire season in the last 100 years, Oregon Public Broadcasting reported October 8. Oregon and Washington have experienced fewer fires than average in 2012, but a record number of acres have burned. A team from the Northwest Interagency Coordination Center, which handles the logistics of fire suppression, presented data on the current fire season to an Oregon senator. Three factors set the stage for larger than usual fires in the northwest. First, in southeast Oregon, very little winter snow and a buildup of grasses and sagebrush contributed to the rapid growth of the Long Draw fire, Oregon's largest fire since 1865, according to the interagency team. Then, in August and September, thousands of lightning strikes ignited two new waves of wildfires across the region, including the Taylor Bridge, which destroyed 61 primary residences. Finally, a summer drought, that continues still, has extended fire season and contributed to the growth of dozens of fires in central and eastern Washington. A meteorologist with the Northwest Interagency Coordination Center said it is unusual for the northwest to have such a dry September. The Forest Service and BLM said so far they have spent about $250 million dollars fighting fires in the northwest in 2012. Source: http://earthfix.opb.org/land/article/wildfires-in-the-northwest-have-burned-record-numb/

Postal and Shipping

(Nevada) **Bomb scare downtown.** A suspected pipe bomb reported by a UPS employee around October 8 prompted police to shut down a major portion of a downtown corridor for several hours in Elko, Nevada. After preliminary examinations, the Elko Bomb Squad decided to detonate the UPS drop-box containing the object. It proved to be "a huge, foot-long bolt, 3/4-inch with a nut on the end, crammed in with the other packages," a police official said. Source: http://elkodaily.com/news/bomb-scare-downtown/article_17dee074-11bf-11e2-ae58-0019bb2963f4.html

(Missouri) **Mail carrier robbed in north St. Louis.** A U.S. Postal Service (USPS) mail carrier was robbed in a north St. Louis neighborhood October 3, the USPS said. The mail carrier was not injured, but a small amount of mail was stolen from her vehicle. The suspect did not display a weapon during the robbery. Source: http://www.ksdk.com/news/article/341529/3/Mail-carrier-robbed-at-gunpoint-

(South Carolina) **UPS driver charged with stealing packages while making deliveries.** A Lancaster, South Carolina driver for United Parcel Service was arrested in September after deputies said she was stealing packages that contained medication, WBTV 3 reported October 3. She was charged with three counts of theft of a controlled substance, according to a news release from the Lancaster County Sheriff's Office. The incidents occurred December 1, 2011, and September 18 and 21, 2012, according to the release. Source: http://www.wbtv.com/story/19725516/ups-driver-charged-with-stealing-packages-while-making-deliveries

Public Health

West Nile outbreak closer to being second worst in U.S. The outbreak of West Nile disease in the United States moved a step closer October 10 to becoming the second worst on record with federal health authorities reporting 280 cases of the virus-caused illness since October 8. There have now been 4,249 cases of West Nile recorded in 2012, according to the Centers for Disease Control and Prevention (CDC), 20 cases fewer than in 2006, the second-largest outbreak on record. The number of deaths rose by five to 168 since October 1, the CDC said. The pace of new cases of the disease has slowed since the summer of 2011. More than 70 percent of the cases have been reported in 8 States: Texas, Mississippi, Michigan, South Dakota, Louisiana, Oklahoma, Illinois, and California. Texas has been the hardest hit, recording close to 40 percent of the cases in the country, according to the CDC. Source: http://articles.chicagotribune.com/2012-10-10/lifestyle/sns-rt-us-usa-health-westnilebre89a03a-20121010_1_neuroinvasive-form-west-nile-outbreaks

Hospital cooperation key to reducing rates of infection, study finds. Based on a new study published October 9 in the journal Health Affairs, researchers from the University of Pittsburgh, Harvard University, and the University of California, Irvine, are urging hospitals to share infection-rate data and adopt the practice of isolating patients carrying methicillin-resistant staphylococcus aureus (MRSA) bacteria. A University of Pittsburgh associate professor of medicine and biomedical informatics said hospitals share patients extensively with other hospitals in their area, facilitating the spread of MRSA infections. The research model demonstrated that a hospital's decision to test patients for MRSA upon admission then isolate those who test positive — a process known as —contact isolation — can help reduce the prevalence of MRSA not only at that location but in other hospitals. Source: http://www.post-gazette.com/stories/news/health/hospital-cooperation-key-to-reducing-rates-of-infection-study-finds-657013/

CDC says 14,000 people at meningitis risk amid call for criminal probe. Health authorities said October 11 that more people than previously thought received possibly tainted steroid injections and that some 14,000 patients could be at risk of contracting meningitis. The Centers for Disease Control and Prevention (CDC) said the number of people at risk, which is 1,000 higher than earlier estimated, was revised after consulting with health authorities. Fourteen patients have died from meningitis and 170 people have been infected, the CDC said in its latest update October 11. The number of infections rose by 33 since October 10, the CDC added.

Florida reported a second death from meningitis and Indiana reported its first death from the outbreak. Meningitis cases have been confirmed in 11 States. State and federal officials are now investigating the New England Compounding Center, which distributed thousands of vials of a contaminated steroid. Five new cases were reported in Tennessee, which remained the hardest-hit State with 49 cases, the CDC said. October 11, Michigan totaled 39 cases, Virginia reached 30, and Indiana's count grew to 21 cases, according to the CDC. Source: http://www.reuters.com/article/2012/10/11/us-usa-health-meningitis-idUSBRE8970TQ20121011

Feds stop Medicare payments after 91 arrests for alleged false billings. Federal authorities have stopped Medicare payments to providers charged in a sweep that netted 91 people in 7 cities accused of $430 million in Medicare billing schemes. The Medicare Fraud Strike Force said operations in Miami, Los Angeles, Dallas, Houston, Brooklyn, New York, Baton Rouge, Louisiana, and Chicago led to the arrests, the largest health care fraud takedown on record, the U.S. Attorney General said October 4. Those arrested allegedly participated in schemes to submit claims to Medicare for treatments that either never happened or were not medically necessary. Patient recruiters, Medicare beneficiaries, and others received cash kick-backs for giving beneficiary information to providers so those providers could submit the false claims, according to court documents. The alleged fraud includes more than $230 million in home health care fraud, more than $100 million in mental health care fraud, and about $49 million in ambulance transportation fraud, the U.S. Attorney General said. Those charged include the owners and operators of 2 different hospitals, 1 in Miami and 1 in Houston, and 16 medical professionals, including 7 physicians, chiropractors, nurses, a psychologist, and a physical therapist. The defendants face various health care fraud charges, including conspiracy to commit health care fraud, health care fraud, violations of the anti-kickback statutes, and money laundering. The Department of Health and Human Services also suspended or took administrative action against 30 health care providers based upon what officials called credible allegations of fraud. HHS can suspend payments until the resolution of an investigation under the Affordable Care Act. Source: http://ifawebnews.com/2012/10/05/feds-stop-medicare-payments-after-91-arrests-for-alleged-false-billings/

Fungal meningitis death toll may rise. Health officials have traced an outbreak of rare fungal meningitis to a Framingham, Massachusetts specialty pharmacy that distributes a steroid injection commonly used to treat back pain, NBC News reported October 4. The pharmacy, which shipped 2,000 vials of the possibly contaminated steroid to one center in Tennessee alone, said it has recalled all of the product and is cooperating with federal officials, said the Associated Press. Doctors leading the investigation said they expect to find more cases, and if the pharmacy shipped product to many States, it is possible many more people across the country will become ill with the hard-to-treat infection. So far, 26 people have been diagnosed with fungal meningitis in 5 States and 4 of them have died. The Massachusetts health department said it was working with federal officials and said the New England Compounding Center had surrendered its license to operate. Source: http://vitals.nbcnews.com/_news/2012/10/04/14219550-fungal-meningitis-death-toll-may-rise?lite

Transportation

Much of odd weapons cache on plane was permissible. Most of the items — including a hatchet and knives — found in the checked luggage of a man taken into custody at Los Angeles International Airport the week of October 1 — would not violate current Transportation Security Administration (TSA) guidelines. The man was stopped during a stopover on a trip from Japan to Boston, when U.S. Customs and Border Protection officers noticed he was wearing a bulletproof vest under his trench coat, along with flame-retardant pants and knee pads. He had reached the United States after a stop in South Korea with a suspicious array of knives and other weaponry in his checked luggage, including a smoke grenade, a biohazard suit, a collapsible baton, masks, duct tape, leg irons, and plastic restraints, authorities said. The smoke grenade was X-rayed by police bomb squad offices in Los Angeles, who said the device fell into a category prohibited on board passenger aircraft. But in Incheon, South Korea, where the man deplaned and went through security, items such as axes, knives, or smoke-generating cartridges are allowed in checked bags, according to a senior airport security official. A U.S. Homeland Security official briefed on the investigation said October 10 South Korean security officials screened the man and his carry-on luggage, but the smoke grenade somehow made it onto the plane. The man was not cooperating with federal officials who are trying to determine why he was headed to Boston with the cache of weapons, authorities said. A former deputy administrator at the TSA said the U.S. will likely look at whether the failure to detect the grenade on a U.S.-bound jet was a one-time lapse or part of a wider security vulnerability. If the U.S. determines a country's airport does not meet U.S. standards, it can ask for stronger security measures and even prohibit flights from flying directly to the U.S. from that country. Source: http://www.azfamily.com/news/national/173648571.html

Water and Dams

(Maine) **Jay police investigate theft of copper valued at $5,000.** Jay police investigated the theft of about $5,000 in used and new copper from the North Jay Water District building in Jay, Maine. A police spokesman told the Lewiston Sun Journal October 11 that the burglary is believed to have occurred October 8 or 9. The copper was reported missing October 10. New rolled copper and an assortment of fittings and some used copper were among the items taken. Source: http://www.pressherald.com/news/maine-Jay-police-investigate-copper-theft-.html

Levees return to pre-flood conditions. The U.S. Army Corps of Engineers believes the Missouri River levee system's protection level is back to what it was before the 2011 flood, KMA 960 AM Shenandoah/99.1 FM Clarinda reported October 8. The 2011 Missouri River flood was the longest-lasting in recorded history, 145 days. It overtopped or breached 157 levees, most of them privately-maintained, and caused millions of dollars damage. However, the damage would have been worse without the levees and the upstream reservoirs that held back even more water. "All the economists tells us $7.6 million dollars worth (of damage) was spared because of that system," said the Corps' district commander. His office oversaw the repairs and rebuilding of the levee system since the official end of the flood October 17 2011. "Eleven of those levees had breaches," he said, "All eleven of those breach locations are back to the level

of protection before the 2011 flood fight." The federal government provides 80 percent funding for districts built to federal standards that are maintained by private sponsors. The districts raise the other 20 percent. Some districts struggled to raise their shares. He credits the State for providing community development block grants to those districts to help reach that match. Without those grants, he said, some repair contracts might not be in place. He said much still needs to be done to repair riverbanks and channel damage and that might take 2 or 3 years to finish. Source: http://kmaland.com/03233_Levees_return_to_pre-flood_conditions_090148.asp

America's levees, dams, navigation projects will decay without new money sources, report says. America's vast network of levees, dams, navigation structures, and hydroelectric power facilities will continue to decay if the federal government does not find new ways to pay to for their maintenance and operation, and fail to prioritize new projects already approved, said a new study released October 4 by the National Academy of Sciences' National Research Council. The report outlines six alternatives for policymakers, many of which call for greater reliance on private funding to maintain the sprawling infrastructure maintained by the U.S. Army Corps of Engineers, including new fees on shippers and manufacturers. Options include to: hike federal funding; decommission or sell parts of the infrastructure overseen by the Corps; boost revenue collected from the beneficiaries of infrastructure projects; and expand partnerships with private industry and local government. The report also calls on the Corps to consider flood-control methods other than building new structures, such as removing or raising existing homes and businesses from flood-prone areas and adopting land use and zoning rules that would avoid new construction. The system the Corps manages was estimated to be worth $237 billion in the 1980s, but is now worth only $164 billion, the study said. Source: http://www.nola.com/environment/index.ssf/2012/10/americas_levees_dams_navigatio.html

(New Jersey) **Tiny parasite is driving $100M plan to replace Garret Mountain reservoirs.** A tiny, waterborne parasite is driving a $100 million plan to replace three reservoirs on Garret Mountain with concrete tanks, the Hackensack Record reported October 4. As New Jersey's Passaic Valley Water Commission (PVWC) moves forward with State approval, there are questions about health risks from the organism in the three reservoirs. The PVWC periodically tests its reservoirs and the Passaic and Pompton rivers for the presence of cryptosporidium (crypto) and giardia. The most recent sampling, conducted September 14, showed the presence of both in the reservoirs, but at low levels that were no cause for alarm. The U.S. Environment Protection Agency standard for water utilities is to remove 99.99 percent of all crypto and giardia from drinking water. The water commission's plan is to drain each of the three reservoirs, beginning with the Levine reservoir in 2014, and then build two low-rise concrete tanks at each reservoir. Source: http://www.northjersey.com/news/environment/Tiny_parasite_is_driving_100M_plan_to_replace_Garret_Mountain_reservoirs.html

Dam inspectors fear the deluge. Extreme weather, shifting demographics, and the passage of time are teaming up to erode the condition of dams and increase the cost of their failure, often measured in millions of dollars and significant numbers of lives lost, the Pew Center of the

States reported October 4. In 2011, States combined to employ just 422 full time workers to oversee 87,679 structures, averaging out to more than 200 per person. Of those dams, 11,388 were deemed —high-hazard, a category quantified differently across States but associated with the likelihood that a failure will lead to fatalities. —They're doing the best job they can. They just don't have the resources, said the executive director of the Association of State Dam Safety Officials. A 2009 study by the group estimated it would cost $16 billion to make the most urgent repairs over the next 12 years. When the Senate reconvenes following the election, it will be asked to consider reviving the 2006 National Dam Safety Act, a measure tacked onto a larger bill that has passed in the House. The $14 million yearly program, which expired in 2011, helped States retain staff, educate dam owners, and buy essential equipment. Since then, funding has trickled in from the Federal Emergency Management Agency, but it has fallen short of plugging the gap. Source: http://www.pewstates.org/projects/stateline/headlines/dam-inspectors-fear-the-deluge-85899420764

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168